Privacy-preserving network monitoring at high-speed

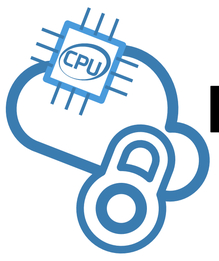
Privacy-preserving network monitoring at high-speed

Thomas Favale (thomas.favale@polito.it)

Supervisors:
Marco Mellia, Idilio Drago, Martino Trevisan

Motivation and background

The analysis of network traffic is essential for many application, such as cyber-security and traffic engineering, but...



Privacy is a critical point

Traffic analyzers must respect Privacy Regulations

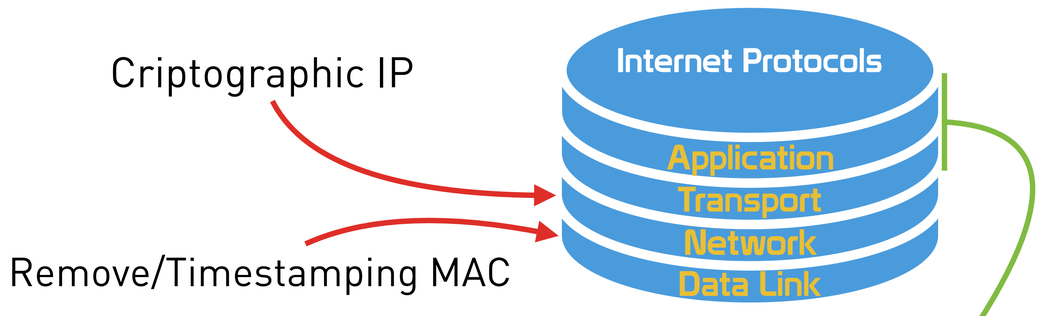
e.g., GDPR

The goal is to perform analysis **without leaking sensitive information**.

Requirements & Configuration

Our solution satisfies **three requirements**:

- It **automatically** searches for protocol fields that can be linked to **particular users**;

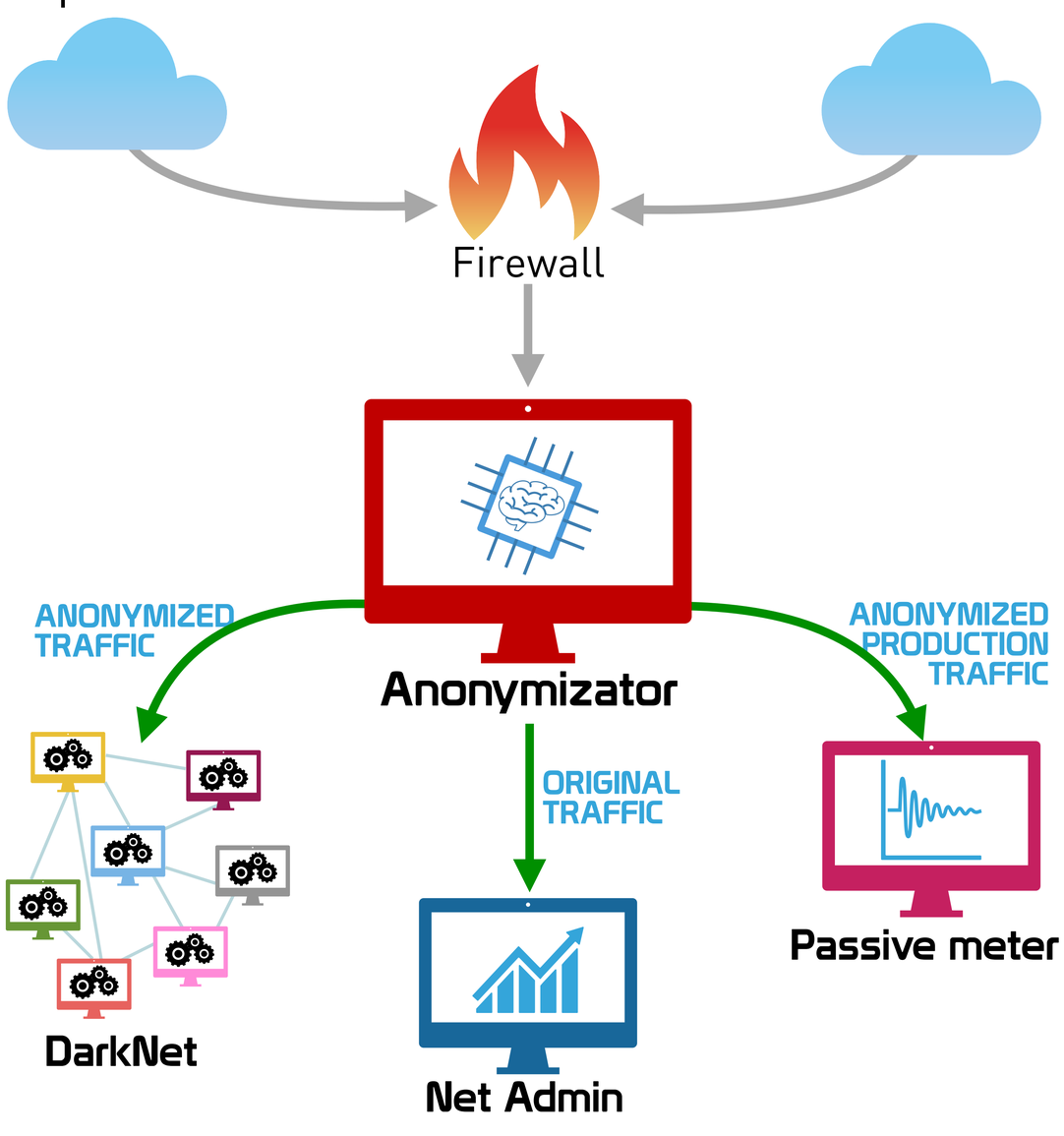


- It anonymizes at **different layers** (e.g. employing **k-anonymization** algorithms)
  - Stateful approach is needed
- It is **light-weight** and **scales with the number of cores**.

Architecture

Our prototype is **deployed** in a **campus network**. It is able to:

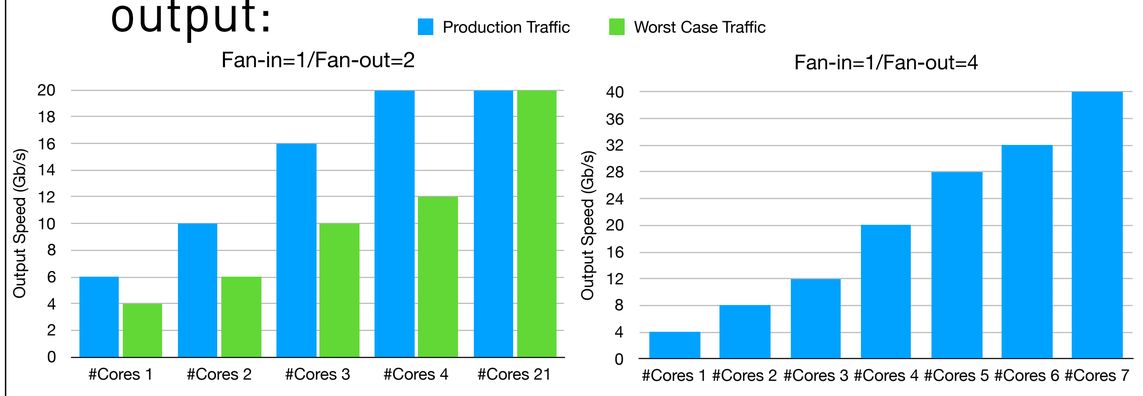
- handle **multiple 10~Gb/s** links with **zero packet loss**;
  - Packet capture based on DPDK
- performing **several anonymization** steps on packets.



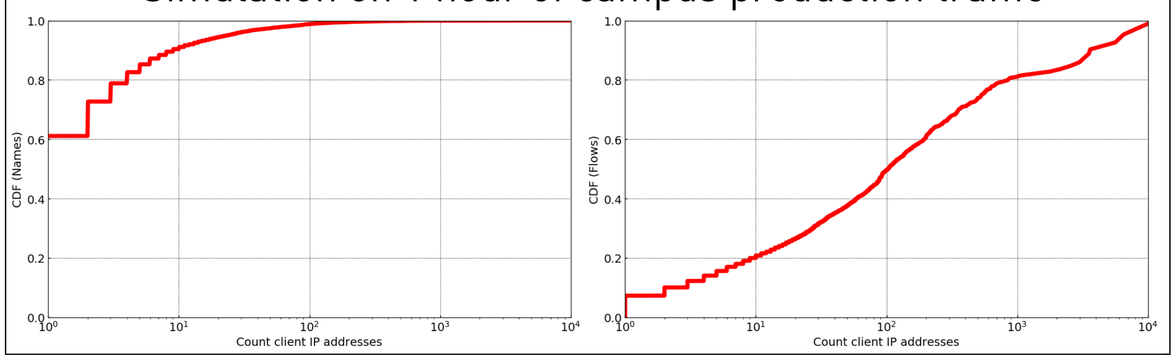
- **Configurable input/output** interfaces

Performance

- Cores required for **20Gb/s** and **40Gb/s** output:



- **K-anonymization** impact on network traffic:
  - Simulation on 1 hour of campus production traffic



Conclusions and future work

- We are implementing **k-anonymization approaches** to perform **selective** anonymization of sensitive fields;
- **Obfuscate** only cases where the **information helps to uncover users** behind the traffic;
- Increase **scalability**;
- **Distributed** architecture.

Open Source